JAN 20 1986

Y1.1/5:99-230

99TH CONGRESS
2d Session

S. RPT.
99-230

FEDERAL GOVERNMENT'S SECURITY CLEARANCE PROGRAMS

COMPLETED

REPORT

MADE BY THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ORIGINAL

JANUARY 22 (legislative day, JANUARY 21), 1986.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1986

BEST COPY AVAILABLE

GPO 27-115

COMMITTEE ON GOVERNMENTAL AFFAIRS

WILLIAM V. ROTH, JR., Delaware, *Chairman*

TED STEVENS, Alaska	THOMAS F. EAGLETON, Missouri
CHARLES McC. MATHIAS, JR., Maryland	LAWTON CHILES, Florida
WILLIAM S. COHEN, Maine	SAM NUNN, Georgia
DAVE DURENBERGER, Minnesota	JOHN GLENN, Ohio
WARREN B. RUDMAN, New Hampshire	CARL LEVIN, Michigan
THAD COCHRAN, Mississippi	ALBERT GORE, JR., Tennessee

FRANKLIN G. POLK, *Chief Counsel and Staff Director*
MARGARET P. CRENSHAW, *Minority Staff Director*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

WILLIAM V. ROTH, JR., Delaware, *Chairman*
WARREN B. RUDMAN, New Hampshire, *Vice Chairman*

CHARLES McC. MATHIAS, JR., Maryland	SAM NUNN, Georgia
WILLIAM S. COHEN, Maine	LAWTON CHILES, Florida
THAD COCHRAN, Mississippi	JOHN GLENN, Ohio
TED STEVENS, Alaska	CARL LEVIN, Michigan
	ALBERT GORE, JR., Tennessee

DANIEL F. RINZEL, *Chief Counsel*
ELEANORE J. HILL, *Chief Counsel to the Minority*
KATHERINE BIDDEN, *Chief Clerk*

BEST COPY AVAILABLE

CONTENTS

	Page
Introduction	1
Witnesses Agreed That Government May Not Be Able to Effectively Clear Over 4.3 Million Personnel	2
Civilian Agencies Highlight Problems With Clearance System	4
Reinvestigation at 5-Year Intervals Applies to Top Secret And SCI but not Secret Clearances	6
DOD Report Highlights Problems in Defense Industrial Security Program	7
Government Found To Be Unable to Verify Assertions Aliens Make About Their Pasts in Countries of Origin	8
Lack of Consistent Standards Reportedly Can Result in Uncertain Clearance Decisions; Centralization, Formal Training Urged	10
Executive Branch Review of Entire Government Personnel Security Program Is Long Overdue	11
Employers Not Held Accountable for Security Breaches	12
Christopher Boyce Warned That Espionage Brings Neither Glamour nor Excitement	13
Technology Is Available That Could Limit Theft, Wrongful Copying of Classified Documents	14
Separate Accounting of Security Costs Proposed as Way To Encourage Defense Contractors to Protect Secrets	15
Privacy Laws Limit Access by DOD, OPM Agents to State and Local Records	16
Hoska Case May Expand Judicial and Regulatory Review of Personnel Issues Affecting National Security	16
Expert Personnel Security Witnesses Called for More Scientific Research	17
Findings, Conclusions, and Recommendations	18

BEST COPY AVAILABLE

99TH CONGRESS
2nd Session

S. RPT.
99-230

FEDERAL GOVERNMENT'S SECURITY CLEARANCE PROGRAMS

JANUARY 22 (legislative day, JANUARY 21), 1986.—Ordered to be printed

Mr. ROTH, from the Committee on Governmental Affairs, submitted the following

REPORT

INTRODUCTION

The Senate Permanent Subcommittee on Investigations held public hearings on the effectiveness of the government's security clearance programs on April 16, 17, 18 and 25, 1985.

The hearings were based on an investigation by the Subcommittee Minority staff under the direction of Senator Sam Nunn, the Ranking Minority Member, and with the concurrence of Senator William V. Roth, Jr., the Chairman.

Noting the necessity for holding these hearings, Chairman Roth said, "Our Nation's first—and strongest—defense against hostile foreign intelligence agents is our people. It is people, not machines, who must safeguard our technology and protect our military secrets. Padlocks, vaults and codes cannot alone keep our secrets safe. We also need a strong program to ensure that those with access are trustworthy and not subject to blackmail and compromise."

Explaining the Subcommittee's interest in personal security, Senator Nunn stated that, "it stems, in part, from our past concern over the transfer of American high technology to the Soviet Union and Soviet Bloc nations. In examining that issue, we found that individuals holding high government security clearances had sold some of this country's most guarded high technology secrets to hostile intelligence services. . . . Such cases suggested critical shortcomings in the government personnel security program and prompted the investigation which led to these hearings."

The investigation and hearings were held under authority of Senate Resolution 354, adopted March 2, 1984, and Senate Resolution 85 of February 28, 1985, both of which direct the Subcommit-

BEST COPY AVAILABLE

tee to examine the efficiency and economy of government operations, including national security programs.

At the hearings, 22 witnesses testified in 450 pages of stenographic transcript with 26 exhibits and 18 statements submitted for the hearing record.

Witnesses Agreed That Government May Not Be Able to Effectively Clear Over 4.3 Million Personnel

The consensus among virtually all of the witnesses was that, in the national security field, too many clearances are requested, too many are granted and that, unless the numbers are reduced substantially, the ultimate result will be a personnel security system of significantly diminished value. As several Senators pointed out, a system that must certify to the reliability of everyone ends up certifying to the reliability of no one.

The latest government-wide figures that we have on security clearances are from 1983, a fact that is significant in itself since it graphically portrays the absence of any centralized authority responsible for our government's security clearance program. The General Accounting Office testified that, as of December 31, 1983, there were approximately 5,116,000 civilian and military personnel, of which 2,725,000, or about 53 percent, had security clearances. This number increased about 7.5 percent from 1982. In addition, over 1,500,000 contractor employees have security clearances. From fiscal year (FY) 1979 through FY 1983 the contractor figure increased by nearly 44 percent.

Those same GAO statistics indicate that of the 3,317,086 uniformed and civilian employees of the Defense Department, 480,363 had top secret clearances. Another 2,066,643 were cleared at the secret level. Some 28,160 had confidential clearances. And 111,167 enjoyed the designation of having sensitive compartmented information, or SCI, access.

Among Defense Department contractor hires, 111,000 employees had top secret clearances, while 900,000 were approved for secret access. Confidential designations numbered 304,800 and SCI access had been given to 10,808. Another 34,397 employees received security clearances from other federal agencies, bringing the total number of individuals holding security clearances to nearly 4.3 million. Moreover, hearing witnesses testified that there was no reason to expect these numbers to decline significantly if present trends continue. In fact, in supplemental testimony, the Defense Investigative Service estimated that the current level of DOD clearances for military, civilian, contractor and reservists is over 4,306,000. Even if there was no change in the number of civilian agency clearances from 1983, this would mean that the current level of government-wide clearances is over 4.6 million employees.

Stressing the magnitude of the challenge of adequately clearing so many employees, Senator Nunn said:

> A sound security clearance program is perhaps more critical to our national security today than ever before in our history. Over 4 million Americans cleared for access . . . are today potential targets for the Soviet KGB. By contrast, the government is already plainly incapable of

BEST COPY AVAILABLE

adequately investigating and reinvestigating all persons seeking security clearances. As we continue to generate more and more highly classified material, our ability to insure selective access to that material is rapidly deteriorating.

DOD officials acknowledged that the sheer magnitude of the numbers of cleared employees presents nearly insurmountable manpower problems at the Defense Investigative Service (DIS), the agency charged with investigating DOD civilian, military and contractor employees requesting clearances. The Office of Personnel Management (OPM) faces similar problems in conducting clearance investigations for employees in the civilian competitive service. OPM Director-designate Donald Devine told the Subcommittee that OPM had experienced a 60 percent increase in investigative workload between 1983 and 1985.

This increase in the number of clearances has contributed to the problem of completing investigations in a timely manner. The General Accounting Office found that the cost to the government caused by delays in processing security clearances is significant. They estimated that in 1982, the cost of lost productivity for just Department of Defense contractor employees awaiting clearance investigations ran as high as $340 million. GAO's best estimate for the current loss in productivity due to clearance delays for the entire Department of Defense (military, civilian and contractor employees) was approximately $850 million per year.

General Richard G. Stilwell, USA (ret.), formerly the Deputy Under Secretary of Defense for Policy and the Pentagon official charged with overseeing the DOD personnel security program,[1] acknowledged that the number of cleared persons was too large. He said the numbers have risen significantly in recent years because of the increased technological level of American weaponry and the accompanying clearance requirements that have been placed on persons designing, constructing and operating such weaponry. An equally important factor in the increase in cleared personnel, he said, was the rapid growth of classified documents. The increase in classified paperwork generated demand for more cleared people to process it. Stilwell said that it would be less difficult to cut the number of persons with clearances than it would be to reduce the number of classified documents. He noted, for example, that Pentagon studies had demonstrated that about one third of the defense contractor employees with top secret clearances do not see top secret information. It was DOD's task to identify more precisely which 33 percent of the top secret clerarance candidates did not actually require such a designation. In addition, he said, the Pentagon was also studying a proposed method of granting a person with a secret clearance a one-time top secret designation when the need for the higher level access clearly would be temporary.

It is important to note that within two months of the conclusion of these hearings, Defense Secretary Weinberger ordered a thorough review of the DOD security clearance process and the reduc-

[1] Subsequent to the hearing, the Secretary of Defense selected General Stilwell to chair a commission to review Department of Defense security policies and programs. The commission is expected to report to the Secretary on its findings in November 1985.

BEST COPY AVAILABLE

tion of total clearances by 10%. The Navy Department, by order of Secretary John Lehman, has likewise begun reducing the number of cleared personnel with a Lehman-set target of 50%. By July, 1985, within a month of the Navy Secretary's order, the number of security clearances in that service had been cut 19% with another 7% of those with access to classified information having their levels of access reduced.

Civilian Agencies Highlight Problems With Clearance System

During the course of the Subcommittee's investigation, a questionnaire on security clearances was forwarded to twenty civilian government agencies.[2] The agencies were chosen because of their diversity in size and operation. Their responses highlighted two of the major complaints leveled at the government's security clearance system.

Agency responses suggested that the system rarely resulted in the denial or revocation of a clearance. The questionnaires requested information on the number of denials and/or revocations of clearances as well as the number of background investigations requested or completed for the period of Fiscal Years 1980 to 1984 inclusive. The results were as follows:

Investigations, fiscal years 1980–84	138,252
Denials/revocations	[1] 118

[1] We cannot tell from many of these responses whether they cover only FY'80 to FY'84 or longer periods. As examples, the Department of Transportation said they only had 6 denials/revocations since DOT was established. Interior stated they had only 6 in the past 14 years. Agriculture said they deny approximately 10 per year but have no accurate records. We converted this to 50 for the time period FY 80–FY 84. GSA was the only agency whose clearance records were limited to the preceding year (reporting 35 denials for FY'84).

Based on those figures, the denial/revocation rate for these civilian federal agencies is approximately .08%. That figure suggests either a deplorable system of investigations and adjudications or the fact that all government employee applicants are amazingly trustworthy.

Another area of concern was information received on the length of time it took OPM to conduct clearance investigations for these agencies. Of the 19 responses, 17 commented negatively on the time it took OPM to do their investigations. OPM has three time categories for conducting background investigations. The projected times are 35 days for expedited cases; 75 days for preappointment cases; and 120 days for postappointment cases. During the past two years, the time factor in the three categores has at least doubled and in some cases tripled. Many of the agencies cited statistics showing the tremendous difference between the time OPM claims they can do investigations and the actual time it takes to do these investigations. These averages are as follows:

---

[2] Of the twenty (20) government entities contacted, nineteen (19) responded. The Civil Aeronautics Board was in the process of ceasing operation and thus was unable to answer our questionnaire. They included: Department of Commerce; Department of Housing and Urban Development; Department of the Interior; Department of Justice; Department of Labor; Department of Transportation; Department of the Treasury; Environmental Protection Agency; U.S. Information Agency; Agency on International Development; Federal Communications Commission; Federal Trade Commission; Commodity Futures Trading Commission; Interstate Commerce Commission; International Trade Commission; General Services Administration; National Aeronautics and Space Administration; Small Business Administration, and Peace Corps.

BEST COPY AVAILABLE

Projected time	*Average actual time*
OPM—120 day investigations	250 days
OPM—75 day investigation	177 days
OPM—35 day investigations	94 days

Such delays were repeatedly cited as causing hardships to the agencies. The Department of the Interior stated that they had experienced the loss or threatened loss of top management candidates due to lagging security investigation time requirements. The Small Business Administration complained that as a result of the delays they were forced to choose between delaying the filling of critical sensitive positions or appointing employees prior to completion of a background investigation. This latter choice not only leads to potential security risks but also, as the Environmental Protection Agency informed the Subcommittee, makes it more difficult to remove that person if the background investigation should develop adverse information. This slow turnaround has even led to problems at NASA in the use of payload specialists (astronauts) who are scheduled for a particular launch date.

The Subcommittee also received testimony from the Department of State and the Nuclear Regulatory Commission (NRC) on the problem of OPM investigative backlog. Both were particularly critical of OPM in the turnaround time of their investigations. Although the Nuclear Regulatory Commission still utilizes OPM, they noted that the delays for such investigations have steadily increased over the last two years. It now averages 270 to 390 days for OPM's 120 day service and 90 to 180 days for OPM's 35 day expedited investigation.

According to the Nuclear Regulatory Commission (NRC):

> (Investigative delays) have had a very adverse impact on NRC's ability to utilize qualified personnel, especially in the scientific and technical disciplines essential to NRC's licensing and regulatory mission. This has resulted in less than fully productive use of many employees (e.g., resident inspectors, or individuals requiring access to classified information) until the completion of the required investigation and grant of security clearance. Resident inspectors serve as the clearest example of this situation since they are not permitted free access to the licensee's nuclear power reactor site until NRC certifies to the licensee that the required investigation as to the inspectors' honesty, trustworthiness and reliability has been conducted and a "Q" security clearance granted to the inspector.

Traditionally, the Department of State relied upon its own resources to conduct all of its background investigations. However, three years ago they began referring a significant amount of the investigations to OPM. Unfortunately, OPM's time service deteriorated to the point at which it was taking 5 to 6 months to complete the investigations. As a result, last year the Department of State stopped referring any investigations to OPM and began contracting out this work to private investigators. On this point, the State Department noted:

> As the result of its contract investigator program, the Department is now able to complete most of its full field

BEST COPY AVAILABLE

> background investigations in approximately 60 days. In that the Department found that in most instances it was able to complete the field investigations before OPM could complete the National Agency Check (NAC); it (the Department) now conducts its own NACs.

In response, OPM witness Donald Devine acknowledged the need for a timely investigative product of high quality. A real problem for OPM in meeting its investigative turnaround goals, according to Mr. Devine, has been the recent surge in numbers of required investigations over the past two years. For example, as noted previously, Devine asserted that, due to a change in contractors at some DOE nuclear facilities and an increase in requests for support by other agencies, OPM has faced a 60% workload increase since 1983, which came after a period of relatively low levels of investigative activity.

To counter the surge-caused delay problem, OPM has instituted a number of administrative changes as well as policy actions within the past two years. They have increased the investigative workforce over the last year and a half, streamlined report formats, accelerated the development of automated processing capability, imposed mandatory overtime requirements, and undertook the innovative approach of using the services of contractor-investigators to help meet surge periods, among other actions.

According to Devine:

> As a result of these actions, I expect to achieve the standard 60 to 65-day turnaround before the end of this calendar year and more importantly, be able to meet future surges and declines in the workloads.

Reinvestigation at 5-year Intervals Applies to Top Secret and SCI but not Secret Clearances

Evidence and testimony at the hearings indicated the need for periodic reinvestigations of cleared personnel. As Bill W. Thurman, Deputy Director of the National Security and International Affairs Division of the General Accounting Office, said:

> Monitoring previously cleared individuals to ensure that their access to classified information remains in the best interest of national security is, or should be, a continuing process.

Similarly, Thomas J. O'Brien, Director of the Defense Investigative Service, testified that the reinvestigation is an essential part of personnel security. He noted that—

> . . . in almost all instances in which cleared people have been found guilty of espionage, it is subsequently determined that they were not involved with foreign intelligence at the time they were investigated and cleared.

Therefore, he concluded, an aggressive reinvestigation program "should serve as a deterrent to those who might otherwise become traitors."

The *Federal Personnel Manual*, issued by the Office of Personnel Management, calls for a reinvestigation every five years for em-

BEST COPY AVAILABLE

ployees with Top Secret or Sensitive Compartmented Information (SCI) clearances or their civilian counterpart designations. While most personnel security experts agree on this requirement, the government is limited in its resources for the task. For example, faced with a large backlog of clearance requests, the Pentagon cut back on reinvestigations in the early 1980s, but currently is conducting them, only on a limited quota basis due to investigative manpower restrictions. It is unlikely that the five-year requirement will be met in the foreseeable future. As GAO's Bill Thurman pointed out, with more than 100,000 individuals with SCI access and about 500,000 with Top Secret clearances in the Defense Department and the defense industry, it may be several years before the Pentagon can get the reinvestigation process on schedule.

The reinvestigation backlog problem is compounded by the fact that the largest population of cleared personnel—those working with Secret clearances—are not included. Secret, the most common of all clearances, has a significance that should not be diminished. Considerable sensitive information can be accessed by persons with Secret clearances. Two well known security violations—the William Holden Bell case and the case involving Ruby Louise Schuler Harper—were both initiated by persons with Secret clearances. Both individuals displayed questionable behavior that might have been detected in reinvestigations. Schuler drank excessively while Bell, embittered on the job and deeply in debt, was seen making purchases and taking vacations suggesting sudden affluence.

In addition, important as the Secret clearence is, the government grants it to persons it does not know very much about. The investigation for a secret clearance generally entails nothing more than a National Agency Check (NAC). Generally, the government will grant a civilian employee a secret clearance when, first, his name does not show up in a derogatory manner in FBI files and other federal agency records; and second, his former employers and teachers, as well as local law enforcement offices where he has lived, have nothing of a serious derogatory nature to say about him. In the case of uniformed military and contractor employees, a secret clearance is generally based only on a check of federal agency files. This information if useful only as the basis of a good start on evaluating the subject's trustworthiness. More information is required, particularly as his career progresses and as his access to sensitive data increases. That is why the reinvestigation, conducted at intervals of no longer than five years, is advocated by experts in the field.

DOD Report Highlights Problems in Defense Industrial Security Program

As part of the hearing record, the subcommittee received the December 1984 Report of the Department of Defense Industrial Security Review Committee, commonly referred to as the "Harper Report." At the request of General Stilwell in the aftermath of the James Harper espionage case, the Committee reviewed and recommended needed improvements in the DOD Industrial Security Program (DISP). That program enforces security requirements for approximately 1.4 million cleared contractor employees and the ap-

BEST COPY AVAILABLE

proximately 16 million classified documents entrusted to their safekeeping.

That report pointed out the very serious difficulties which the government faces in clearing massive numbers of contractor employees. Many of these problems mirror those encountered in clearing government employees, including:

—Manpower shortages at DIS in the face of an incredibly huge workload in the contractor sector: requests for contractor clearances run as high as 26,000 per month;

—Given DIS manpower, it would take DIS an entire decade to perform the 280,000 clearance investigations required for contractor personnel as of the end of 1984;

—The single largest category of industrial clearances are those 900,000 employees holding Secret clearances. The report found current procedures for granting secret clearances "to be among the weakest aspects of the Industrial Personnel Security Program" and noted that today thousands of persons have access to Secret materials based only on national agency checks conducted more than twenty years ago;

—Despite manpower shortages, clearances are requested for large numbers of contractor personnel who do not require access to classified information—citing plumbers, electricians and custodial personnel as common examples;

—of the 115,000 contractor personnel with Top Secret clearances, 90,000 to 95,000 do not have frequent access to Top Secret material and 35,000 to 40,000 have *never* had access to Top Secret material.

To correct these and other problems, the report concluded with twenty-five recommendations for improvements, including reduction in the number of industrial clearances, revisions in the scope of clearance investigations, centralization of clearance adjudication within the Defense Department, stricter controls on after-hours access to cleared facilities, and the establishment of a National Industrial Security Hotline.

Government Found To Be Unable To Verify Assertions Aliens Make About Their Pasts in Countries of Origin

At the hearings, the Subcommittee examined the procedures the government follows when immigrant aliens and recently naturalized citizens apply for U.S. security clearances. The Subcommittee sought to determine how thorough an inquiry the government conducts into a clearance applicant's past in the country of his birth and in other foreign nations in which he may have lived before settling here.

The Subcommittee had special interest in immigrant aliens and recently naturalized citizens who came to this country from Communist nations and other closed societies such as Libya and Iran and who have gotten jobs in the national security field. Clearly, the vast majority of the immigrants who have come to this country from closed societies have been loyal, dedicated and talented members of the national community. They have made many valuable contributions to the development of the United States over the years. There remain, however, serious difficulties in the procedures

BEST COPY AVAILABLE

by which the government investigates foreign-born applicants for security clearances. Testimony by the FBI and other agencies and by the Subcommittee staff indicated that little of the information the foreign-born give about themselves can be verified in clearance investigations. This applies not only to Communist and closed societies but, to varying degrees, to Western nations and other democracies.

Testifying for the FBI, Philip A. Parker said the Bureau had no authority to conduct personnel security background investigations overseas. Parker, Deputy Director of the FBI's Intelligence Division, said that when the Bureau is asked to do a background inquiry on a foreign-born clearance applicant it "must rely on whatever information is provided" by the host country. That may vary from country to country, he said, adding, "we are not in a position to verify or otherwise confirm" assertions the clearance applicant has made about himself in his personnel security forms. He said the FBI was "completly dependent" on the host country as to the extent of cooperation given in personnel inquiries of this type.

Investigating the issue of clearances for new arrivals to this country, the Subcommittee Minority staff under Senator Nunn studied the immigration and security clearance procedures followed in the case of Panagiotis Takis Veliotis, a Greek shipping executive who emigrated to Canada in the early 1950s and later to the United States. As an official of the General Dynamics Corporation, he was placed in charge of several national defense programs, including construction of the Trident submarine and the Los Angeles class SSN nuclear attack submarine. For nearly a year Veliotis served as President-Manager at a facility handling classified military and nuclear work, despite the fact that Veliotis himself held no security clearance. He later received Secret and Top Secret Pentagon clearances and a "Q" clearance from the Energy Department.

The Minority staff found that the government was unable to verify even the most simple assertions Veliotis made about his life in Greece, including information about his birth, formal education, military service and lack of a criminal record. A. Barry Dalinsky, Deputy Director of Security for the Department of Energy, agreed that the Veliotis clearance investigation was clearly inadequate, calling the case "an excellent example of how failure to follow established procedures can lead to questionable adjudication." The potential harm to national security in placing someone with unverified credentials in a sensitive job was made even more worrisome by the fact that Veliotis has now fled the United States to avoid having to face a federal grand jury indictment charging him in a multi-million dollar kickback scheme.

In light of the problems highlighted by the *Veliotis* case, the staff recommended that the Departments of State, Defense and Energy, the Office of Personnel Management and the intelligence community work together to devise a more reliable system of doing personnel security checks in foreign countries on immigrant aliens and recently naturalized citizens.

BEST COPY AVAILABLE

Lack of Consistent Standards Reportedly Can Result in Uncertain Clearance Decisions; Centralization, Formal Training Urged

Hearing testimony underscored the need for greater consistency in the investigation and adjudication of clearances throughout the government. Background investigations conducted by different agencies for the same level clearance vary in scope; the standards vary by which different agencies grant or deny the same level clearance.

Part of the problem stems from the lack of a formal training program for personnel security adjudicators, those persons who, after reviewing background investigations, decide whether or not to grant a candidate's clearance request, or to revoke or maintain an incumbent worker's clearance. The Defense Investigative Service, a component of the Defense Department and the agency which conducts almost all personnel security inquiries, has a formal training program for its agents. But no such educational procedure is available for civilian or military adjudicators, most of whom learn their skills on the job.

GAO has been advocating more consistent standards for both investigators and adjudicators for eight years. GAO's position, put forward at the hearings by Thurman, is that investigations and adjudications are not evaluated according to the same criteria throughout the government. As a result, persons denied clearances by one agency may be able to obtain them at others. He noted, for example, that DIS agents, required to undergo formal training, are sometimes better qualified in personnel security matters than are agency program security officers. Citing the need for formal training for adjudicators as well as street agents, Thurman went on to say—

> . . . the establishment of consistent standards for investigations and adjudications cannot be fully effective unless the investigators and adjudicators are properly trained. Although useful guidance on personnel investigations and adjudications is available, we believe that personnel involved in these activities still need formal training government-wide. Such training would provide greater assurance that the investigative and adjudicative processes are performed in a professional and consistent manner that protects the interests of the government and the interests of the subjects of the investigation in a fair and equitable manner.

In the case of contractors working on Special Access Programs (SAP) or Sensitive Compartmented Information (SCI) procurements, inconsistencies in overall security requirements may also be considerably burdensome. Lawrence Howe, Vice President, Corporate Security for Science Applications International Corporation, testified that his company is now "running upwards of 30 different industrial security program," all required by what amounts to a single customer: the United States Government. At the least, within the Department of Defense, security requirements, includ-

BEST COPY AVAILABLE

ing clearance investigation and adjudication, should be consolidated.

Executive Branch Review of Entire Government Personnel Security Program Is Long Overdue

During the year-long investigation leading up to the April hearings, it became apparent that a complete study of the entire government personnel security program by the Executive Branch was long overdue.

On March 11, 1983 the President, via the National Security Decision Directive on Safeguarding National Security Information (NSDD–84), requested the Attorney General, in consultation with the Office of Personnel Management, to establish a group to study the entire federal personnel security program and recommend appropriate revisions in existing Executive Orders, regulations and guidelines. After consultation with OPM, the Department of Justice convened a group consisting of representatives of the Office of Personnel Management, Department of Defense, Department of Energy, Department of Treasury, and the Federal Bureau of Investigation.

Preliminary meetings of this interagency group identified several fundamental policy issues relating to the government's personnel security program. On May 1, 1984, guidance from the National Security Council was sought on these issues in order for the interagency group to proceed in an expeditious and efficient manner. Although a number of participants in the interagency group have repeatedly contacted the National Security Council (NSC) for a response, none has been forthcoming. Thus, since May 1, 1984, this long-needed Executive Branch review of the government's clearance system has been forestalled, pending action by the National Security Council.

In the interim, the Office of Personnel Management issued, on January 6, 1984, a new set of personnel security and suitability guidelines commonly referred to as Basic Installment 311 of the Federal Personnel Manual. Director-designate Devine of OPM testified at the hearings that these guidelines were intended to collect and organize the various regulations governing the existing programs, a task that had not been performed for 15 years prior to the issuance of the Basic Installment 311.

Director-designate Devine, however, testified that any changes under Basic Installment 311 that could have bound the agencies concerned suitability issues only and that the agencies, including the Department of Defense, had agreed that the NSDD–84 process would not address suitability but that OPM would retain authority in that area.

Unfortunately, a number of agencies, including the Department of Defense, disagreed, claiming that the guidelines did in fact affect security determinations. They viewed the new guidelines as premature at best and counterproductive at worse. With more than a million DOD civilian positions affected by the 311 series, the Department of Defense complained that the guidelines were issued without their prior consultation and coordination and would be tremendously cost ineffective. The Department of Defense also believed

BEST COPY AVAILABLE

these guidelines to be premature since the NSDD-84 study group had not issued its final recommendations on personnel security. Apparently as a result of this controversy between DOD and OPM over Basic Installment 311, the 98th Congress exempted DOD from these guidelines in the FY 1985 Defense Authorization bill.

The delays surrounding the NSDD-84 study group proposals and the continuing dispute regarding Basic Installment 311 raise again the need for an overall review of the government's personnel security programs. The preliminary recommendations by the NSDD-84 interagency group include an effort to create uniform and consistent investigative and adjudicative standards for national security matters as well as uniform and consistent investigative and adjudicative standards for suitability matters. Ideally, the agencies involved should be applying consistent standards for personnel security decisions in a coordinated and efficient manner.

Given the critical importance of the personnel security program, the NSDD-84 recommendations should be given prompt attention by the National Security Council.

Subsequent to the hearing, Congress addressed this problem, requiring the National Security Council to respond to the NSDD-84 study group proposals. On July 30, 1985, the Senate approved the Defense Authorization Act for F.Y. 1986, which included conference committee language, proposed by Rep. Patricia Schroeder (D-Colo.) and Senator Nunn, that requires the National Security Council to respond to the interagency group's recommendations within 60 days of enactment of the Act. The legislation further requires the interdepartmental group to report its findings and recommendations to Congress within 90 days of the date on which the requested guidance is provided by the National Security Council. The provision also calls for the transfer of all authority relating to suitability and security assigned to the Director of the Office of Personnel Management, to the Secretary of Defense unless the President specifically directs that they remain with OPM before the interagency group reports to Congress. The House approved this legislation on October 29, 1985 and was approved by the President on November 8, 1985 (Public Law 99-145).

Employers Not Held Accountable for Security Breaches

The Subcommittee received evidence and testimony about several major security compromises, including three that took place in the private sector—the James Durward Harper-Ruby Schuler case, the Christopher Boyce-Andrew Daulton Lee case and the William Holden Bell case.

In each of these cases, information was developed indicating that the compromises occurred at times when the firms that employed the violators could have enforced stricter adherence to security procedures.[3]

---

[3] The need for effective personnel security programs was again highlighted shortly after the hearings with the May and June 1985 arrests on espionage charges of retired Navy Warrant Officer John Walker, Jr.; his son, Yeoman 3rd Class Michael Lance Walker; John Walker Jr.'s brother, retired Navy Lieutenant Commander Arthur Walker; and retired Navy radioman Jerry Whitworth.

BEST COPY AVAILABLE

In the Harper-Schuler case, for example, Schuler maintained her Secret clearance despite the fact that she was known to be drinking heavily and spending money well beyond her known means. A more alert personnel security program at her business, Systems Control, Inc., of Palo Alto, California, might have identified her as a possible security problem. As a contractor in the Defense Industrial Security Program, Systems Control was required to report any untoward conduct on a cleared employee's part to the Pentagon. No such report was made.

Similarly, Christopher Boyce, a highly cleared communications clerk in a CIA-sponsored secret project at a TRW plant in Redondo Beach, California, was able to smuggle sensitive documents out of the facility in part because of inadequate or unenforced security procedures. Boyce, who gave these documents to his friend Daulton Lee for delivery to KGB agents in Mexico City, said drinking and other irresponsible behavior were commonplace in sections of the plant which had been cordoned off because of the sensitivity of the data being processed there. Several of Boyce's allegations about TRW security procedures, including weak supervision, drinking, and poor control of badge material, were confirmed in the government inspection following his arrest.

William Holden Bell, a radar specialist at Hughes Aircraft, sold sensitive information about classified weapons systems, including the "quiet radar" system utilized on the B–1 and Stealth bombers, to Polish spies. Bell appeared as a witness before the Subcommittee during the course of its May 1982 hearings on the Transfer of High Technology to the Soviet Union. He testified that, while employed at Hughes, he had "all the signals, all the classical reasons" for being a spy, including financial difficulties, followed by sudden affluence, job dissatisfaction, and close friendship with a Polish national. None of these potential "indicators" were reported by his employer to DIS.

In none of these cases was the employing firm held accountable for the conduct of its employees. No fines were levied and business with federal agencies went on as before, as if the contractors were not responsible in any way for the conduct of their employees.

Christopher Boyce Warned That Espionage Brings Neither Glamour nor Excitement

Now serving a 68-year prison sentence for espionage, escape and bank robbery, Christopher Boyce was convicted in 1977 of what is considered one of the most serious national security compromises in recent years. Disillusioned at age 21 by, among other things, Vietnam, Watergate, and a President's resignation, Boyce delivered highly secret information about CIA surveillance satellite programs to his boyhood friend, drug dealer Andrew Daulton Lee, for sale to Soviet agents in Mexico City.

In his testimony, Boyce related in detail those lax security practices which, in his words, "were a great help to me in compromising a CIA project to the Russians." His description of regular consumption of alcohol and "partying" in a highly secret "black vault" at TRW underscored the importance of strong and effective security programs at the contractor level.

BEST COPY AVAILABLE

In closing, Boyce stressed what he felt remains the most critical problem in personnel security: the failure of the government to impress upon the public the tragic personal consequences of espionage. He suggested that strict security regulations are "next to worthless if each of the four million Americans with security clearances do not have a grasp of how espionage would affect them personally."

Boyce was troubled by his belief that cleared personnel view espionage as an enticing escapade in glamour and intrigue. Based on his own experience, he knew that nothing could be farther from the truth:

> . . . there was no excitement; there was no thrill. There was only depression and a hopeless enslavement to an inhuman, uncaring foreign bureaucracy. I hadn't made myself count for something. I had made my freedom count for nothing.

Boyce tried in his testimony to express to other government and defense contractor employees the pain and suffering his conduct had caused him. He said there may be other cleared personnel who may be considering espionage. It may seem romantic or adventuresome, he said, but the price he paid for the experience was far greater than he had anticipated when he first became involved.

He offered these words of caution to cleared personnel who may be thinking about signing on with the KGB:

> As we sit here a half dozen, perhaps a dozen, perhaps more Americans, are operatives of the KGB. Perhaps some of them have been in place for years. I tell you that none of them are happy men or women. And I would suspect that there are hundreds of other Americans out of the 4 million with security clearances who have given serious thought to espionage. Those are the people that you must seek out and reach with the truth. It is infinitely better for you to make the extra effort to ensure that your personnel understand beyond a shadow of a doubt how espionage wounds a man than for more and more of them to find out for themselves. No American who has gone to the KGB has not come to regret it. For whatever reason a person begins his involvement, a week after the folly begins, the original intent and purpose becomes lost in the ignominy of the ongoing nightmare. Be it to give your life meaning or to make a political statement. Be it to seek adventure or to pay your delinquent alimony. Be it for whatever reason, see a lawyer or a psychiatrist or a priest or even a reporter, but don't see a KGB agent. That is a solution to nothing.

Technology Is Available That Could Limit Theft, Wrongful Copying of Classified Documents

While TRW Vice President Paul W. Schwegler testified that the firm had corrected security shortcomings that Boyce had exploited in the 1970s, the Subcommittee sought the views of other witnesses as to how to further improve plant safeguards against espionage.

BEST COPY AVAILABLE

Representing the 3M Corporation of St. Paul, Minnesota, Marketing Director P.J. Muldowney told the Subcommittee that the application of new document control technology could benefit government officials and defense contractor firms trying to secure classified documents.

Muldowney, in a statement submitted for the hearing record, said classified documents can be electronically labelled in such a manner so as to cause photocopiers to sound an alarm when they are copied. In addition, he said, a system of electronic detection devices can be set up at building entrances and exits that will signal alarms when these same labelled documents are carried in clothing, purses, briefcases and layers of other documents through wired passageways.

Such a system controlling photocopying and passage would have served to deter not only Boyce but also William Holden Bell and Ruby Louise Schuler and other violators whose theft and reproduction of sensitive documents have been uncovered in recent years, Muldowney said. He added that his firm and others have the technology needed to install such systems in the buildings of defense contractors and government.

Stressing his view that this technology will not prevent espionage, but would limit the damage violators could inflict, Muldowney explained:

> . . . we do not have the panacea. It is difficult to imagine that it will ever be accomplished. The professional spies have a variety of devices at their disposal. What we do have is the best deterrent available to prevent the proliferation of unauthorized copies and their removal from controlled environment.

Separate Accounting of Security Cost Proposed as Way To Encourage Defense Contractors To Protect Secrets

Lawrence Howe, an executive in a private firm that conducts research and development for the armed services and industry, also proposed creation of an accounting incentive that would encourage defense contractors to improve their security procedures. Money spent on better security should be identified as such and should not be combined with other contract costs, Howe said. With such a distinction, he explained, contractors could strengthen their personnel and plan safeguards against espionage while still keeping down their production costs.

"There is a paradox in the case of the contractor who expends sufficient resources to implement a high quality security program," Howe testified, pointing out that such a contractor may come in with a higher—and losing—bid while the company that neglects its security procedures can submit a schedule of lower costs. "The contractor who reduces the impact on overhead rates by the least possible expenditure on security has a competitive advantage under present contract award evaluation procedures," Howe said. "For this reason, contractor security managers are under pressure to meet only minimum requirements. This results in the expenditure of as little resource as possible."

BEST COPY AVAILABLE

Privacy Laws Limit Access by DOD, OPM Agents to State and Local Records

Agents conducting personnel security investigations for the Pentagon and the Office of Personnel Management are doing important work. In every personnel inquiry they undertake, the nation's security may ultimately be involved. Testimony before the Subcommittee indicated that privacy legislation and other statutes and regulations have had the effect on denying or significantly limiting agents' access to law enforcement and criminal justice records at the state and local level. Massachusetts and California, for example, along with several other states, have privacy laws which limit DOD and OPM agents' access to personal information held by local, county and state governments.

Defense Investigative Service Director O'Brien has called for remedial legislation requiring state and local authorities to grant federal clearance investigators access to criminal justice information. Absent such legislation, the federal government remains unable to accurately determine facts that seem essential to any worthwhile security investigation: whether an individual seeking access to national security information has any prior record of criminal conduct.

Subsequent to the hearing, legislation designed to correct this problem has been proposed in the Senate. On June 25, 1985, Senator Nunn introduced S. 1347, the Security Clearance Information Act of 1985, joined by Senators Roth, Lawton Chiles (D-Fla.), Albert Gore, Jr. (D-Tenn.) and Ted Stevens (R-Alaska). If enacted into law, this legislation would authorize the federal government to obtain access to state and local criminal justice records when conducting eligibility investigations for (1) access to classified information, (2) assignment to or retention in sensitive national security duties, or (3) acceptance or retention in the armed services. The bill was referred to the Senate Governmental Affairs Committee for consideration.

At the urging of Senator Nunn, on June 27, 1985, the Senate Armed Services Committee amended S. 1271, the Intelligence Authorization Act for F.Y. 1986, by adding language similar to that proposed in S. 1347. The amended version of S. 1271 subsequently passed both Houses of Congress and became law on December 4, 1985 (Public Law 99-169).

Hoska Case May Expand Judicial and Regulatory Review of Personnel Issues Affecting National Security

The Subcommittee reviewed the *Hoska* v. *U.S. Army* case and its possible long range implications for government personnel security programs. Pentagon spokesmen and other officials are concerned that the *Hoska* case may have the effect of reducing personnel security decisions to the level of employee grievance disputes.

Lukas E. Hoska, a civilian Intelligence Operations Specialist in the Army, was found to be emotionally unstable and guilty of security violations and bad judgment. In reaching this assessment about the man four years after it hired him, the Army took away his Top Secret clearance and, then, because his work required such a clearance, fired him.

BEST COPY AVAILABLE

Hoska appealed. On April 30, 1982, the U.S. Court of Appeals for the District of Columbia declared that even where no constitutional issue was involved, a court could review a security clearance decision by the Army. In *Hoska,* the court found the Army's determination to be wrong and ordered that Hoska's Top Secret clearance be reinstated and that he be given his job back.

As a federal civilian employee whose job had been lost along with his clearance, Hoska had first appealed his case to the Merit Systems Protection Board, a quasi-judicial tribunal for employee grievences. Kathleen A. Buck, Assistant General Counsel in the Pentagon, testified that because of this ruling both the courts and the U.S. Merit Systems Protection Board may now intervene in personnel security matters affecting national security, even in cases where there are no constitutional issues. This is an unprecedented and unfortunate development, Buck said, pointing out that Pentagon officials are trained to decide personnel security matters affecting national security. Judges and Merit Systems Protection Board members and staff, she said, are not trained to carry out this duty.

Buck warned:

> If the *Hoska* case remains intact and is relied upon by other courts as a precedent, I believe the courts and the Merit Systems Protection Board will be second guessing agencies on the issue of whether an individual applicant for a security clearance is trustworthy. I foresee the courts not only substituting their judgment for agency decisions to revoke or deny a clearance, but also substituting their personal opinions for agency decisions on what positions require security by ensuring the trustworthiness of empoyees who work with classified information or in classified areas is slowly being usurped by the judiciary and the MSPB.[4]

Expert Personnel Security Witnesses Called for More Scientific Research

The need to increase research efforts in personnel security was cited by two personnel security experts at the hearings. Eli S. Flyer, a consultant to the Navy, and Lawrence J. Howe both called for more study into the kinds of persons likely to collaborate with hostile intelligence services. Flyer and Howe advocated more scientific research into the profile of a traitor.

"While large investments have been made by the military services in behavioral science research to evaluate and improve personnel selection, assignment, training and utilization procedures," Flyer testified, "there has been little involvement by Defense scien-

[4] In an opinion issued subsequent to the hearing, the Merit Systems Protection Board reconsidered the impact of the *Hoska* case. In *Egan* v. *Department of the Navy,* issued August 8, 1985, the Board held that in an adverse action over which the Board has jurisdiction and which is based substantially on the agency's revocation or denial of a security clearance, the Board has no authority to review the agency's stated reasons for the security clearance determinations. Under the *Egan* decision, the Board will review: (1) the requirement of a security clearance for the position; (2) the loss or denial of the security clearance; and (3) the granting of minimal due process protections to the employee. The Board also held that its authority does not extend to ordering the agency to reinstate an employee's security clearance.

BEST COPY AVAILABLE

tists in the research needed to evaluate and improve security investigations."

Similarly, Howe advocated research into the personality traits that persons who commit espionage may share with people guilty of more predatory crimes. "The profile of a traitor may not be significantly different from that of many sociopaths and felons," he said. "Loyalty to country has become so abstract that an act of treason is not necessarily different from any other serious crime. What differentiates a traitor from a common thief may be little more than opportunity. The existing and extensive studies on criminal behavior need to be reviewed from the clearance viewpoint for insight. At present there is insufficient focus on this important resource."

Findings, Conclusions, and Recommendations

1. The government's personnel security program should be devoted to accurately detecting potential security risks as well as efficiently clearing large numbers of personnel.

2. The number of personnel holding clearances for access to highly sensitive information must be reduced. Our current system cannot adequately insure the continued integrity and reliability of the 4.3 million Americans who today hold security clearances. Furthermore, hearing testimony strongly suggested that many of those 4.3 million have no actual need for a security clearance. Clearance requests have reached unmanageable numbers, resulting in diluted investigative resources and background investigations of diminished quality. The President should issue an executive order directing that government agencies and contractors substantially cut the number of security clearances within 2 years with a goal of a 50% reduction. As an added incentive, those agencies and contractors who make the largest cuts should be given priority on remaining clearance requests.

3. Complementing the reduction in clearances, there must also be a significant effort to insure that information is classified only where truly necessary to maintain the national security. Although the Subcommittee's investigation did not focus in detail on the problem of overclassification, the 1984 report of the Information Security Oversight Office, released shortly after the Subcommittee's hearings, confirmed that "overclassification" of information remains a problem within the government.

4. The National Security Council should promptly complete its review of the personnel security programs. Although the National Security Council has been charged with initiating needed reforms in personnel security, this had not been accomplished at the time of the hearings. Given the critical importance of these reforms to our national security, the National Security Council should act promptly and without further delay, to carry out this responsibility. Absent such action, Congress will be forced to consider enacting legislation to replace, revise, and consolidate the dated executive orders which now govern the government's security clearance programs.

5. An executive body should be established with personnel security oversight responsibilities for the entire government similar to

BEST COPY AVAILABLE

those which the Information Security Oversight Office now holds for the classification of information. This organization should specify and enforce uniform government-wide standards for security investigations and adjudications for both personnel and facility clearances. Standard requirements for formal training for both investigators and adjudicators should be established.

6. Congress must also focus on problems dealing with classified information in the legislative branch. For the most part, there are no established standards or procedures. Personal offices and Committee practices vary widely in terms of their handling of clearances and classified material. There are few, if any, checks in this system. We believe an overall review of security procedures in the legislative branch should be conducted by the Rules Committee in consultation with the Intelligence Committee with a goal of recommending improvements where needed. We commend the Senate Intelligence Committee's efforts in this area and recommend the review of their practices and procedures as a model for such improvements. Senators Roth and Nunn have addressed this issue through preliminary letters to the Senate leadership.

7. A more thorough quality background investigation should be conducted on those individuals with Secret clearances who have access to highly sensitive information. Hearing testimony established, without dispute, that the national agency check, currently used as the basis for most Secret clearances, is woefully inadequate as a background investigation. Some effort should be made to review and perhaps restructure the massive Secret clearance category with a view to prioritizing those clearances actually affecting the most critical and sensitive information.

8. There should be regular periodic reinvestigations of personnel with Secret and Top Secret clearances. Timely reinvestigation should be considered as important and be accorded as much priority as the initial background investigation. Cleared employees, at both government and contractor levels, should be required to complete periodic updated personnel security questionnaires. Some responsibility for updates should be shifted where possible to the users' security departments.

9. More realistic sanctions, such as debarment, suspension, and the imposition of monetary fines, should be meted out to employers of cleared personnel, including defense contactors, if they knowingly or through negligence violate personnel security regulations. Greater emphasis should be placed on the use of these sanctions in an effort to increase the accountability of contractors for security violations.

10. Legislation should be enacted which would allow security clearance investigative agencies such as the Defense Investigative Service and the Office of Personnel Management to obtain needed background information from criminal justice agencies at the state and local level as well as private corporations. Currently, they are often refused needed information due to interpretations of a variety of laws, including state privacy acts, the federal privacy act, and the Fair Credit Reporting Act. S. 1347, introduced in the Senate by Senators Nunn and Roth on June 25, 1985, is designed to correct this problem.

BEST COPY AVAILABLE

11. An interagency group should be formed to develop a more effective means for conducting personnel security investigations regarding immigrant aliens and recently naturalized citizens who apply for security clearances. U.S. agencies which assist in clearance investigations abroad should recognize the critical importance of this task to national security and prioritize their efforts accordingly.

12. Responsible government agencies should increase efforts in the area of personnel security research to develop appropriate investigative strategies and procedures and to identify, where possible, areas of personnel vulnerability. Hearing testimony indicated that, at least in the Defense Department, there has been no significant dedication of resources for furthering study in this area, despite its growing importance to our national security.

13. Congress should consider the need for legislation clearly specifying that the Merit Systems Protection Board is authorized to review employment, as opposed to security, decisions. The Board, whose expertise does not encompass questions of national security, should not be engaged in the denial or reinstatement of security clearances.

14. The government should determine the feasibility of utilizing available technology for the encoding of classified documents to prevent their unauthorized duplication and removal. If feasible, this technology should be implemented as soon as possible on, at the least, a prioritized basis determined by the sensitivity and vulnerability of the material involved.

15. Continuing security awareness programs on behalf of federal agencies and industrial contractors should be given the highest priority. These programs should emphasize the harsh realities and grave personal consequences of espionage in an attempt to dispel popular misconceptions of espionage as an often glamorous and intriguing adventure.

16. Within the Department of Defense, all industrial clearance adjudication, including Special Access Programs (SAP) or Sensitive Compartmented Information (SCI) procurements, should be consolidated. According to hearing testimony, the present division of adjudication authority generates inconsistency, unpredictability and duplication of effort within the Department of Defense clearance system.

17. Under current rules, contractors who reduce security costs have a competitive advantage in the bidding process. Current Federal Acquisition Regulations should be reviewed to determine whether they can be modified to segregate security costs from those overhead rate determinations used for the award of contracts. Testimony suggested that the current inclusion of security costs in overhead gives contractors a "disincentive" to strengthen and improve security programs.

18. Defense Investigative Service (DIS) and Office of Personnel Management (OPM) investigators are not currently authorized to use the National Crime Information Center (NCIC) data bank. Law enforcement agencies routinely use that data bank to quickly obtain updated criminal record information. The Attorney General should proceed with arrangements for both the defense Investigative Service and Office of Personnel Management to be granted

BEST COPY AVAILABLE

access to the National Crime Information Center by the Board of Governors. Use of the Center would greatly facilitate access to state criminal records which are often otherwise unavailable for use in clearance investigations.

19. Government agencies and contractors should emphasize and strictly adhere to the "need to know" standard in submitting clearance requests. Greater responsibility should be delegated to the employers of cleared personnel, including contractors, to "prescreen" individuals submitted for clearances. In order to strengthen their incentive to eliminate unnecessary clearances, the costs of investigations conducted by the Defense Investigative Service should be charged to the appropriate DOD service or agency, similar to the system now employed by the Office of Personnel Management. Contractors should be charged for the cost of any DIS investigations requested beyond established quotas for those requests. Under current rules, costs of Defense Investigative Service investigations are covered by the DIS budget, rather than by those agencies requesting the investigations.

20. The requirements for cleared personnel and facilities vary in response to federal budget priorities. To meet uneven demand, the Office of Personnel Management and the Department of State have instituted plans of contracting with experienced outside investigators who can be called upon during surge periods, thus delivering adequate investigative products without unnecessarily expanding the permanent federal workforce. All agencies responsible for conducting personnel security investigations should examine the feasibility of, and consider, following this procedure during surge periods.

21. Currently, only three professional employees in the Department of Defense are responsible for policy operations for what amounts to the largest personnel security program in the Free World. More realistic staffing would help eliminate the need to periodically create oversight committees to propose reforms of the program. The office in DOD dealing with personnel security policy should be given enhanced status and adequately staffed and funded so that it can effectively oversee the DOD personnel security program.

22. In keeping with these recommendations, the Subcommittee commends the work of the Department of Defense Industrial Security Review Committee as set forth in its December 1984 report. The Committee's analysis of the Defense Industrial Security Program was extremely helpful to the Subcommittee in identifying and examining major shortcomings within the program. The Subcommittee recommends that the Department of Defense review and implement where feasible the Committee's recommendations for improvement of the Industrial Security Program, with particular emphasis on those portions dealing with the enhancement of personnel security investigative standards; the reduction of industrial clearances; increased and improved security requirements for industrial contractors—including strict monitoring of after-hours access; and revision of the industrial security inspection system.

○

BEST COPY AVAILABLE